

Review of Claim Language

Each of the claims are directed to a unified communication system (or unified communications server) that receives a key from a requesting device, as part of a user interface session, in order to cause at least one of encryption or decryption of a message. In particular, each of the independent claims 1, 11, 22, 30, 37, 47, 58, and 68 specify: (1) receiving *from a requesting device* a request for providing (i.e., generation of) a user interface session; (2) generating for the requesting device as part of the user interface session a prompt for the *user of the requesting device to input a key* (e.g., an encryption key for sending a message, or a decryption key for retrieval of a message); (3) invoking a resource configured for executing encryption or attempted decryption of the message based on the key received from the requesting device as part of the user interface session.

Hence, each of the independent claims explicitly specify that the *unified communications system / server* invokes the resource configured for executing encryption or attempted decryption of the message.

In addition, the independent claims explicitly specify that encryption/attempted decryption by the invoked resource is based on the encryption key/decryption key that *is input by the user* via the requesting device *as part of the user interface session*.

Hence, each of the independent claims enable a user of the requesting device to send and/or receive encrypted messages, *regardless of whether any encryption / decryption utility is installed on the requesting device* that is in use by the user, based on prompting the user for an encryption/decryption key *as part of the user interface session*, and receiving the encryption/decryption key *as part of the user interface session*.

These and other features are neither disclosed nor suggested in the applied prior art.

Claims 1, 22, 37, and 58

A. U.S. Patent No. 6,442,600 to Anderson

1) No User Interface Session

Applicant traverses the Examiner's assertion that Anderson discloses any type of "user interface session" between a requesting device and the claimed unified communications system / server. Anderson provides no disclosure or suggestion whatsoever of the claimed "user interface session": as described in the specification (e.g., page 9, lines 8-15) and explicitly recited in the claims, the "user interface session" requires multiple transactions between the unified communications system and the requesting device (e.g., receiving message, generating first and second prompts, and reception of the encryption key *as part of the user interface session* in claims 1, 22, 37, and 58).

Hence, the broadest reasonable interpretation cannot be inconsistent with the specification or the explicit claim language, which requires multiple transactions between the unified communications system and the user interface device.

Anderson describes a system for "distributing electronic messages" (see Abstract) that comprises (see Fig. 1) multiple "recipient *client* computer systems 150 160, 170, 180 suitable for receiving and sending electronic messages" (e.g., col. 4, lines 61-63) and a "server computer system 100" that sends and receives electronic messages from the recipient client computer systems 150, 160, 170, and 180.

All interactions by the user are with the corresponding recipient computer system (e.g., 150), and not the server computer system 100. For example, col. 5, lines 12-18 describe with respect to Fig. 1 that each recipient computer system 150 includes a Message Sender 154 and a Message Receiver 155, and that recipient computer system 150 also can store the server system's public key 157. Further, col. 5, lines 19-35 describes that "[u]se of the [Message Distribution Server] MDS system begins when a user (e.g., a user of a recipient computer system) uses a Message Sender to supply an electronic message to the MDS system" (col. 5, lines 18-21). Fig. 3 illustrates the operations by the Message Sender implemented in the recipient computer system, which includes retrieval of the locally stored server's public key 157 (of Fig. 1, col. 5, lines 15-

16) in step 320, encryption by the Message Sender in step 320, and sending the message in step 330 to the server 100 for distribution (col. 8, lines 34-51).

Hence, all user interactions in requesting encryption of a message to be sent are with the recipient computer system (i.e., the “requesting device”).

There is no action performed by the server computer system 100 on a transmitted message until the message is received by the server 100. See, e.g., col. 5, lines 36-37 (“[w]hen the MDS system receives a message to be distributed...”); col. 8, lines 57-63 (describing operations in server 100 with respect to Fig. 4, where “[t]he routine begins at step 405 *where a new message is received ...*”, and Fig. 5 illustrates no interaction by the Message Distributor in the server 100 with sending client computer 150).

Hence, there is no interaction whatsoever in Anderson that could be considered a teaching or suggestion of the claimed “user interface session” that enables a user to request encryption, as specified in independent claims 1, 22, 37, and 58.

2) No Generating For the Requesting Device a First Prompt to Select Encryption, or Invoking a Resource for Executing Encryption, by the System / Server

Applicant further traverses the assertion that Anderson teaches a unified communications system / server / device executing a medium that generates *for the requesting device* as part of the user interface session a first prompt enabling the user to select encryption of the message. As described above, Anderson provides no user interface session between the system / server and the *requesting device*.

Rather, Anderson teaches that all operations are performed in the requesting device by the message sender 154. As described above, each recipient computer system 150 includes a Message Sender 154 and can store the server system’s public key 157. Fig. 3 illustrates operations by the message sender routine, including determining in step 315 “whether the user has indicated to encrypt the message” (col. 8, lines 43-44); if encryption is selected, the Message Sender retrieves the locally stored server’s public key, and the Message Sender *in the requesting device* encrypts the message in step 320 with the locally-retrieved server’s key. The Message

Sender then sends the message to the server in step 330 (see col. 5, lines 12-20 and 25-30; col. 8, lines 42-47).

Hence, Anderson neither discloses nor suggests that the unified communications system / server / device executing the medium generates *for the requesting device* a first prompt.

In fact, Anderson never generates a first prompt enabling the user to select encryption, but rather **detects** whether the user has **already** selected encryption (see, e.g., col. 5, lines 25-26 “[t]he *sender can also indicate* whether the message should be transmitted in an encrypted manner”; col. 8, lines 43-44 “[i]n step 315 it is determined whether the user has indicated to encrypt the message.”): this is not a teaching of generating a first prompt (let alone by a server), but simply a detection of whether the user has selected encryption. Regardless, these operations are performed in the requesting device, and not in the server, as claimed.

In fact, the Examiner admits on page 3 that Anderson does not teach “a second prompt for the user to supply an encryption key”, or “encrypting the message based on the encryption key received from the requesting device.” Hence, the assertion by the Examiner that Anderson teaches “invoking a resource configured for executing encryption of the message into an encrypted message based on the encryption key” is inconsistent with the Examiner’s admission that Anderson does not teach “encrypting the message based on the encryption key received from the requesting device.”

B. U.S. Patent No. 5,870,477 to Sasaki

The Examiner asserts that Sasaki teaches “symmetric encryption of a message where a user inputs an encryption key for encrypting a centrally stored data/message. and where a select number of receivers are able to decrypt the data/message” (citations omitted).

This assertion, however is unsubstantiated, as Sasaki provides no reference whatsoever to the term “symmetric encryption”.

Further, the assertion does not resolve the Examiner’s admissions on page 3 that Anderson does not teach “a second prompt for the user to supply an encryption key”, or “encrypting the message based on the encryption key received from the requesting device.”

Rather, the Examiner's assertion simply addresses "the user to supply an encryption key" and "encrypting the message based on the encryption key", while disregarding the explicit claim limitation that *encryption* is based on the *encryption* key is *received from the requesting device*.

Therefore, the rejection is legally deficient because it fails to address the claimed feature of the system/ server / device generating the second prompt *for the requesting device*, or that the encryption is performed based on the encryption key *received from the requesting device*.

Moreover, Sasaki also teaches that all encryption is performed in the client device (e.g., computer system 1 of Fig. 1, sending station 74 of Fig. 31). Column 41, line 46 to col. 42, line 20 explicitly require that the client device perform all encryption. As noted by the Examiner, Sasaki teaches with respect to Fig. 31 that a management key MA is sent by the sending station 74 to the receiving stations 75 and 77, but not the mail server 70 (col. 41, line 65 to col. 42, line 20). Hence, Sasaki teaches that it is impossible for the mail server 70 to either encrypt or decrypt any message!

C. The Hypothetical Combination of Anderson, Sasaki, and Gifford

Hence, neither Sasaki or Anderson, singly or in combination, disclose or suggest that the unified communications system / server / device executing the medium invokes the resource for executing encryption based on the encryption key *received from the requesting device*, as claimed.

In fact, both Anderson and Sasaki consistently require that the *client device* perform the encryption. Given that Gifford is silent on how to perform any encryption, the hypothetical combination of Anderson, Sasaki, and Gifford still would require the encryption to be performed in the client device sending the message to the server.

Hence, the hypothetical combination neither discloses nor suggests the claimed unified communications system / server / device executing the medium executing the operation of invoking a resource configured for executing encryption of the message based on the encryption key *received from the requesting device*.

For these and other reasons, the rejection of independent claims 1, 22, 37, and 58 should be withdrawn.

Claims 11, 30, 47, and 68

A. Anderson

1) No User Interface Session

As described above, Anderson provides no disclosure or suggestion of the claimed “user interface session”, which requires multiple transactions between the requesting device and the unified communications system /server: claims 11, 30, 47, and 68 explicitly specify that the user interface session is to enable a user to retrieve stored messages, generate a prompt for the messaging subscriber to input a decryption key, and supply of the decryption key by the messaging subscriber *as part of the user interface session*.

Anderson provides no interaction between the server system 100 and the requesting device that can be considered a teaching of the claimed “user interface session”. Figs. 4 and 6 illustrate that a “request” from a message recipient results in a corresponding operation be performed by the Message Tracker Routine (Fig. 6) based solely on the request (e.g., deleting a message, set a save flag, or sending a retrieved message to recipient).

In fact, the Examiner admits on page 8 that Anderson fails to teach “generating a prompt ... to input a decryption key”, or “the decryption key having been supplied ... as part of the user interface session.” Hence, the Examiner’s admission is inconsistent with the assertion that Anderson teaches the “user interface session”, as specified in claims 11, 30, 47, and 68.

2) No Subscriber Profile Directory

Applicant traverses the assertion that Anderson teaches “accessing, for the user interface session, subscriber profile information *from a subscriber profile directory*”: the Examiner’s citation of “column 6, lines 5-67” fails to identify any reference whatsoever to the claimed subscriber profile directory. In fact, the cited portion provides no reference whatsoever to any data structure that can be considered a “subscriber profile directory”.

B. Sasaki

As admitted on page 8 of the Official Action, Anderson neither discloses nor suggests “generating a prompt based on identifying the one stored message as encrypted, for the messaging subscriber to input a decryption key; and invoking a resource configured for attempting decrypting of the one stored message based on the decryption key having been supplied by the messaging subscriber via the requesting device as part of the user interface session.”

The Examiner asserts that Sasaki teaches “symmetric encryption of a message where a user inputs an **encryption key for encrypting a centrally stored data / message**, and where a select number of **receivers are able to decrypt** the data/message by inputting a decryption key and **performing decryption of the message**.” (Citations omitted)

As apparent from the assertion by the Examiner (and the foregoing description of Sasaki with respect to claims 1, 22, 37, and 58), the rejection is legally deficient because it fails to address the claimed “generating a prompt ... for the messaging subscriber to input a decryption key”, and the claimed **system / server / device executing the medium** “invoking a resource configured for attempting decrypting ... based on the decryption key having been supplied *by the messaging subscriber via the requesting device*”, as claimed.

Rather, Sasaki teaches with respect to Fig. 31 (col. 41, line 45 to col. 42, line 20) that the receiving devices 75 and 77 receive the management key MA **from the sending station 74** (col. 41, lines 62-67); the receiving devices 75 and 77 read the enciphered file 1 (and including enciphered mail A and enciphered key KA) generated by the sending station 74 from the mail center 70, and the receiving devices 75 and 77 perform decryption **using the supplied management key MA from the sending station 74** (col. 42, lines 13-20).

Hence, Sasaki provides no disclosure or suggestion whatsoever of the claimed “generating a prompt ... for the messaging subscriber to *input a decryption key*”, because Sasaki explicitly teaches that the decryption key is **received from the sending station 74**.

In fact, Sasaki teaches that the decryption is performed exclusively in the receiving devices: it is impossible for the mail center 70 to invoke a resource for attempted decryption because the management key MA is never sent to the mail center 70.

Hence, none of the applied references of Anderson, Sasaki, or Gifford disclose or suggest that the unified communications system / server / device executing the medium invokes a resource for attempted decryption based on: (1) generating a prompt for the *requesting device* for the messaging subscriber to input a decryption key, let alone (2) invoking a resource for attempting decrypting based on the decryption key having been supplied by the messaging subscriber *via the requesting device*.

For these and other reasons, the §103 rejection of the independent claims 11, 30, 47, and 68 should be withdrawn.

Conclusion

It is believed the remaining dependent claims are allowable in view of their dependency from the respective independent claims.

The Examiner acknowledged during a telephonic interview on April 21, 2006 that the prior rejections in the October 3, 2005 Office Action were not moot, but were overcome in view of Applicant's January 3, 2006 response.

In view of the above, it is believed this application is in condition for allowance, and such a Notice is respectfully solicited.

To the extent necessary, Applicant petitions for an extension of time under 37 C.F.R. 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including any missing or insufficient fees under 37 C.F.R. 1.17(a) or 1.17(e), to Deposit Account No. 50-1130, under Order No. 95-456, and please credit any excess fees to such deposit account.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'L R Turkevich', with a stylized flourish at the end.

Leon R. Turkevich
Registration No. 34,035

Customer No. 23164
Date: July 18, 2006